



**March 28, 2023**

Challenge yourself with our [Fraud Prevention Quiz!](#)

[This past week's stories:](#)

 [Report finds leaks in Halifax Water cybersecurity systems](#)

 [Only 9 per cent of Canadian firms are cyber mature: Cisco report](#)

 [Safety Net: How a devastating cyberattack on Newfoundland's health-care system is prompting changes across Canada](#)

[From ransomware to cyber espionage: 55 zero-day vulnerabilities weaponized in 2022](#)

[ChatGPT bug leaked users' conversation histories](#)

[North Dakota is first state to approve required cybersecurity education](#)

[German and South Korean agencies warn of Kimsuky's expanding cyber attack tactics](#)

[14 million customer details breached in Latitude financial firm](#)

[Casino operator Crown Resorts faces major cyber attack](#)

[2023 Cybersecurity Maturity Report reveals organizational unpreparedness for cyberattacks](#)

[OpenAI reveals Redis bug behind ChatGPT user data exposure incident](#)

[North Korean hackers play the 'long con' by targeting experts](#)

---

### **Report finds leaks in Halifax Water cybersecurity systems**

An audit of Halifax Water by the Halifax Regional Municipality's auditor general has found deficiencies in the utility's cybersecurity, including employees clicking links in emails.

<https://www.cbc.ca/news/canada/nova-scotia/auditor-general-water-utility-cybersecurity-systems-1.6791236>

*Click above link to read more.*

[Back to top](#)

---

## **Only 9 per cent of Canadian firms are cyber mature: Cisco report**

Only nine per cent of companies in Canada and 13 per cent in the U.S. have a mature level of preparedness to face cyber attacks, according to a Cisco Systems estimation.

<https://www.itworldcanada.com/article/only-9-per-cent-of-canadian-firms-are-cyber-mature-cisco-report/533964>

*Click above link to read more.*

[Back to top](#)

---

## **Safety Net: How a devastating cyberattack on Newfoundland's health-care system is prompting changes across Canada**

Health-care providers have some of your most private information in their databases. A detailed list of all your ailments, the drugs you're taking, your identification and contact information – and there's a good chance a cybercriminal is trying to steal it all for a quick buck.

<https://financialpost.com/cybersecurity/cyberattack-newfoundland-healthcare-prompts-changes-across-canada>

*Click above link to read more.*

[Back to top](#)

---

## **From ransomware to cyber espionage: 55 zero-day vulnerabilities weaponized in 2022**

As many as 55 zero-day vulnerabilities were exploited in the wild in 2022, with most of the flaws discovered in software from Microsoft, Google, and Apple.

<https://thehackernews.com/2023/03/from-ransomware-to-cyber-espionage-55.html>

*Click above link to read more.*

[Back to top](#)

---

## **ChatGPT bug leaked users' conversation histories**

A ChatGPT glitch allowed some users to see the titles of other users' conversations, the artificial intelligence chatbot's boss has said.

<https://www.bbc.com/news/technology-65047304>

*Click above link to read more.*

[Back to top](#)

---

## **North Dakota is first state to approve required cybersecurity education**

North Dakota is the first state in the nation to approve legislation requiring cybersecurity education.

<https://www.kxnet.com/news/state-news/north-dakota-is-first-state-to-approve-required-cybersecurity-education/>

*Click above link to read more.*

[Back to top](#)

---

## **German and South Korean agencies warn of Kimsuky's expanding cyber attack tactics**

German and South Korean government agencies have warned about cyber attacks mounted by a threat actor tracked as Kimsuky using rogue browser extensions to steal users' Gmail inboxes.

<https://thehackernews.com/2023/03/german-and-south-korean-agencies-warn.html>

*Click above link to read more.*

[Back to top](#)

---

## **14 million customer details breached in Latitude financial firm**

The personal information of 14 million Australians and New Zealanders was stolen as a result of a serious security breach. Systems at consumer lending company Latitude Group revealed on Monday that the information had been stolen from them after a theft discovered two weeks prior.

<https://informationsecuritybuzz.com/customer-details-latitude-financial/>

*Click above link to read more.*

[Back to top](#)

---

## **Casino operator Crown Resorts faces major cyber attack**

Crown Resorts said a ransomware group had contacted the company, claiming that they had gained access to some files related to Australia's biggest casino operator following a data breach at a file transfer service GoAnywhere.

<https://infotechlead.com/security/casino-operator-crown-resorts-faces-major-cyber-attack-77551>

*Click above link to read more.*

[Back to top](#)

---

## **2023 Cybersecurity Maturity Report reveals organizational unpreparedness for cyberattacks**

In 2022 alone, global cyberattacks increased by 38%, resulting in substantial business loss, including financial and reputational damage. Meanwhile, corporate security budgets have risen significantly because of the growing sophistication of attacks and the number of cybersecurity solutions introduced into the market. With this rise in threats, budgets, and solutions, how prepared are industries and countries to effectively address today's cyber risk?

<https://thehackernews.com/2023/03/2023-cybersecurity-maturity-report.html>

*Click above link to read more.*

[Back to top](#)

---

## **OpenAI reveals Redis bug behind ChatGPT user data exposure incident**

OpenAI on Friday disclosed that a bug in the Redis open source library was responsible for the exposure of other users' personal information and chat titles in the upstart's ChatGPT service earlier this week.

<https://thehackernews.com/2023/03/openai-reveals-redis-bug-behind-chatgpt.html>

*Click above link to read more.*

[Back to top](#)

---

## North Korean hackers play the 'long con' by targeting experts

Bruce Klingner, a longtime Northeast Asia specialist, once received a message from a verified email address of Korea analyst Aidan Foster-Carter that seemed innocuous: Would Klingner review a paper by nuclear policy expert Jamie Kwong?

<https://www.washingtonpost.com/world/2023/03/28/north-korea-hackers-phishing-attack/>

*Click above link to read more.*

[Back to top](#)

---

Click [unsubscribe](#) to stop receiving the Digest.

\*\*\*\*\*  
\*\*\*\*\*

The Security News Digest (SND) is a collection of articles published by others that have been compiled by the Information Security Branch (ISB) from various sources. The intention of the SND is simply to make its recipients aware of recent articles pertaining to information security in order to increase their knowledge of information security issues. The views and opinions displayed in these articles are strictly those of the articles' writers and editors and are not intended to reflect the views or opinions of the ISB. Readers are expected to conduct their own assessment on the validity and objectivity of each article and to apply their own judgment when using or referring to this information. The ISB is not responsible for the manner in which the information presented is used or interpreted by its recipients.

For previous issues of Security News Digest, visit the current month archive page at:

<http://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/security-news-digest>

To learn more about information security issues and best practices, visit us at:

<https://www.gov.bc.ca/informationsecurity>

[OCIOSecurity@gov.bc.ca](mailto:OCIOSecurity@gov.bc.ca)

The information presented or referred to in SND is owned by third parties and protected by copyright law, as well as any terms of use associated with the sites on which the information is provided. The recipient is responsible for making itself aware of and abiding by all applicable laws, policies and agreements associated with this information.

We attempt to provide accurate Internet links to the information sources referenced. We are not responsible for broken or inaccurate Internet links to sites owned or operated by third parties, nor for the content, accuracy, performance or availability of any such third-party sites or any information contained on them.

